=> d ibib 1-5

PCTFULL   COPYRIGHT 2001 MicroPatent
ACCESSION NUMBER: 2000047600 PCTFULL   EW 200033   ED 20000904
TITLE (ENGLISH):   PHOTO-INDUCED NUCLEIC ACID **HYBRIDIZATION**
TITLE (FRENCH):   HYBRIDATION D'ACIDES NUCLEIQUES PAR PHOTO-INDUCTION
INVENTOR(S):   AL-SHEIKHLY, Mohamad; BENTLEY, William, E.; SILVERMAN,
                         Joseph

PATENT ASSIGNEE(S):   AL-SHEIKHLY, Mohamad; BENTLEY, William, E.; SILVERMAN,
                         Joseph

LANGUAGE OF PUBL.:   English
LANGUAGE OF FILING: English
DOCUMENT TYPE: Patent
PATENT INFORMATION:

                         NUMBER   KIND   DATE

                         WO 2000047600   A1 20000817
DESIGNATED STATES: AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE
                         DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE
                         KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX
                         NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA
                         UG US UZ VN YU ZA ZW GH GM KE LS MW SD SL SZ TZ UG ZW
                         AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR
                         GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW
                         ML MR NE SN TD TG
APPLICATION INFO.:   WO 2000-US3357   20000210
PRIORITY (ORIGINAL):   US 1999-60/119417   19990210
                         US 1999-60/136185   19990527

ACCESSION NUMBER: 2000:146535   USPATFULL
TITLE: Compositions for sorting **polynucleotides**
INVENTOR(S):   Brenner, Sydney, Cambridge, United Kingdom
PATENT ASSIGNEE(S):   Lynx Therapeutics, Inc., Hayward, CA, United States
                         (U.S. corporation)

                         NUMBER   KIND   DATE
                         ----------------- ------ --------
PATENT INFORMATION: US 6140489   20001031
APPLICATION INFO.:   US 1998-183650   19981030   (9)
RELATED APPLN. INFO.:   Continuation of Ser. No. US 1995-485105, filed on 7 Jun
                         1995, now patented, Pat. No. US 5863722 which is a
                         continuation of Ser. No. US 1994-359295, filed on 19
                         Dec 1994, now patented, Pat. No. US 5695934 which is a
                         continuation-in-part of Ser. No. US 1994-322348, filed
                         on 13 Oct 1994, now abandoned
DOCUMENT TYPE: Utility
FILE SEGMENT: Granted
PRIMARY EXAMINER: Elliott, George C.
ASSISTANT EXAMINER: Shibuya, Mark L.
LEGAL REPRESENTATIVE: Macevicz, Stephen C.
NUMBER OF CLAIMS: 7
EXEMPLARY CLAIM: 1
NUMBER OF DRAWINGS: 5 Drawing Figure(s); 4 Drawing Page(s)
LINE COUNT: 1794
CAS INDEXING IS AVAILABLE FOR THIS PATENT.

ACCESSION NUMBER: 1999:12739   USPATFULL
TITLE: Method of sorting **polynucleotides**
INVENTOR(S):   Brenner, Sydney, Cambridge, England
PATENT ASSIGNEE(S):   Lynx Therapeutics, Inc., Hayward, CA, United States

(U.S. corporation)

	NUMBER	KIND	DATE
PATENT INFORMATION:	US 5863722		19990126
APPLICATION INFO.:	US 1995-485105		19950607 (8)

RELATED APPLN. INFO.: Continuation of Ser. No. US 1994-359295, filed on 19
Dec 1994 which is a continuation-in-part of Ser. No. US
1994-322348, filed on 13 Oct 1994, now abandoned

DOCUMENT TYPE:	Utility
FILE SEGMENT:	Granted
PRIMARY EXAMINER:	Chambers, Jasemine C.
ASSISTANT EXAMINER:	Priebe, Scott D.
LEGAL REPRESENTATIVE:	Macevicz, Stephen C.
NUMBER OF CLAIMS:	14
EXEMPLARY CLAIM:	10
NUMBER OF DRAWINGS:	7 Drawing Figure(s); 6 Drawing Page(s)
LINE COUNT:	1785

CAS INDEXING IS AVAILABLE FOR THIS PATENT.

ACCESSION NUMBER:	97:115100 USPATFULL
TITLE:	Massively parallel **sequencing** of sorted **polynucleotides**
INVENTOR(S):	Brenner, Sydney, Cambridge, England
PATENT ASSIGNEE(S):	Lynx Therapeutics, Inc., Hayward, CA, United States (U.S. corporation)

	NUMBER	KIND	DATE
PATENT INFORMATION:	US 5695934	·	19971209
APPLICATION INFO.:	US 1994-359295		19941219 (8)

RELATED APPLN. INFO.: Continuation-in-part of Ser. No. US 1994-322348, filed
on 13 Oct 1994, now abandoned

DOCUMENT TYPE:	Utility
FILE SEGMENT:	Granted
PRIMARY EXAMINER:	Chambers, Jasemine C.
ASSISTANT EXAMINER:	Priebe, Scott D.
LEGAL REPRESENTATIVE:	Macevicz, Stephen
NUMBER OF CLAIMS:	23
EXEMPLARY CLAIM:	12
NUMBER OF DRAWINGS:	7 Drawing Figure(s); 6 Drawing Page(s)
LINE COUNT:	1787

CAS INDEXING IS AVAILABLE FOR THIS PATENT.

PCTFULL   COPYRIGHT 2001 MicroPatent

ACCESSION NUMBER:	1996012039 PCTFULL
TITLE (ENGLISH):	MASSIVELY PARALLEL **SEQUENCING** OF SORTED **POLYNUCLEOTIDES**
TITLE (FRENCH):	**SEQUENCAGE** MASSIVEMENT PARALLELE DE **POLYNUCLEOTIDES** TRIES
INVENTOR(S):	BRENNER, Sydney
PATENT ASSIGNEE(S):	LYNX THERAPEUTICS, INC.
LANGUAGE OF PUBL.:	English
DOCUMENT TYPE:	Patent
PATENT INFORMATION:	

NUMBER	KIND	DATE
WO 9612039	A1	19960425

DESIGNATED STATES:	AU CA CZ FI HU JP KR NO SG AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT
APPLICATION INFO.:	WO 1995-US12678 19951012

L11   ANSWER 1 OF 9   BIOSIS   COPYRIGHT 2002 BIOSIS   DUPLICATE 1
ACCESSION NUMBER: 2001:541615 BIOSIS
DOCUMENT NUMBER: PREV200100541615
TITLE: Evolutionary HMMs: A Bayesian approach to multiple
                    alignment.
AUTHOR(S):   Holmes, Ian (1); Bruno, William J. (1)
CORPORATE SOURCE: (1) Group T10, Los Alamos National Laboratory, Los Alamos,
                    NM, 87545 USA
SOURCE: Bioinformatics (Oxford), (September, 2001) Vol. 17, No. 9,
                    pp. 803-820. print.
                    ISSN: 1367-4803.
DOCUMENT TYPE: Article
LANGUAGE: English
SUMMARY LANGUAGE: English

AB   Motivation: We review proposed syntheses of **probabilistic**
     sequence alignment, profiling and phylogeny. We develop a multiple
     alignment **algorithm** for Bayesian inference in the links model
     proposed by Thorne et al. (1991, J. Mol. Evol., 33, 114-124). The
     algorithm, described in detail in Section 3, samples from and/or
     maximizes the posterior distribution over multiple alignments for any
     number of DNA or protein **sequences,** conditioned on a
     phylogenetic tree. The individual sampling and maximization steps of the
     algorithm require no more computational resources than pairwise
     alignment. Methods: We present a software implementation (Handel) of our
     algorithm and report test results on (i) simulated data sets and
     (ii) the structurally informed protein alignments of BAliBASE (Thompson et
     al., 1999, Nucleic Acids Res., 27, 2682-2690). Results: We find that the
     mean sum-of-pairs **score** (a measure of residue-pair
     correspondence) for the BAliBASE alignments is only 13% lower for Handel
     than for CLUSTALW (Thompson et al., 1994, Nucleic Acids Res., 22,
     4673-4680), despite the relative simplicity of the links model (CLUSTALW
     uses affine gap **scores** and increased penalties for indels in
     hydrophobic regions). With reference to these benchmarks, we discuss
     potential improvements to the links model and implications for Bayesian
     multiple alignment and phylogenetic profiling.

L11   ANSWER 2 OF 9   CAPLUS   COPYRIGHT 2002 ACS
ACCESSION NUMBER: 2001:656508   CAPLUS
TITLE: Statistical significance of **probabilistic**
                         sequence alignment and related local hidden
                         Markov models
AUTHOR(S):   Yu, Yi-Kuo; Hwa, Terence
CORPORATE SOURCE: Department of Physics, Florida Atlantic University,
                         Boca Raton, FL, 33431-0991, USA
SOURCE: J. Comput. Biol. (2001), 8(3), 249-282
                         CODEN: JCOBEM; ISSN: 1066-5277
PUBLISHER: Mary Ann Liebert, Inc.
DOCUMENT TYPE: Journal
LANGUAGE: English

AB   The **score** statistics of **probabilistic** gapped local
     alignment of random **sequences** is investigated both anal. and
     numerically. The full **probabilistic algorithm** (e.g.,
     the "local" version of max.-likelihood or hidden Markov model method) is
     found to have anomalous statistics. A modified "semi-
     probabilistic" alignment consisting of a hybrid of Smith-Waterman
     and **probabilistic** alignment is then proposed and studied in
     detail. It is predicted that the **score** statistics of the hybrid
     algorithm is of the Gumbel universal form, with the key Gumbel
     parameter .lambda. taking on a fixed asymptotic value for a wide variety
     of **scoring** systems and parameters. A simple recipe for the

computation of the "relative entropy," and from it the finite size
correction to .lambda., is also given. These predictions compare well
with direct numerical simulations for **sequences** of lengths
between 100 and 1,000 examd. using various PAM substitution **scores**
and affine gap functions. The sensitivity of the hybrid method in the
detection of **sequence** homol. is also studied using correlated
sequences generated from toy mutation models. It is found to be
comparable to that of the Smith-Waterman alignment and significantly
better than the Viterbi version of the **probabilistic** alignment.

REFERENCE COUNT: 47
REFERENCE(S):
(1) Altschul, S; J Mol Biol 1990, V215, P403 CAPLUS
(3) Altschul, S; Methods Enzymol 1996, V266, P460 CAPLUS
(4) Altschul, S; Nucl Acids Res 1997, V25, P3389 CAPLUS
(6) Altschul, S; Proteins 1998, V32, P88 CAPLUS
(10) Bucher, P; Comput Chem 1996, V20, P3 CAPLUS
ALL CITATIONS AVAILABLE IN THE RE FORMAT

ACCESSION NUMBER: 2001:43683   CAPLUS
DOCUMENT NUMBER: 135:103309
TITLE: DNA sequencing with transposons
AUTHOR(S):   Cawley, Simon E.; Speed, Terence P.
CORPORATE SOURCE: Department of Statistics, University of California, Berkeley, CA, 94720-3860, USA
SOURCE: J. Comput. Biol. (2000), 7(5), 717-729
                       CODEN: JCOBEM; ISSN: 1066-5277
PUBLISHER: Mary Ann Liebert, Inc.
DOCUMENT TYPE: Journal
LANGUAGE: English

AB   The use of transposons offers the possibility of a directed approach to
DNA sequencing, where a target DNA up to about 6kb in length can be
sequenced quickly and with minimal redundancy. Transposons are mobile DNA
elements which can be inserted in a reasonably random fashion into the
target DNA. An important part of this process is the location of the
transposon insertions (known as mapping) and the selection of a sensible
subset of transposons to use as priming sites for sequencing reactions.
This paper presents a **probabilistic** method of **scoring**
selected subsets of transposons and a graph-theoretic **algorithm**
for selection of a subset of maximal **score**.

REFERENCE COUNT: 13
REFERENCE(S):
(1) Adams, M; Science 2000, V287, P2185
(2) Berg, C; Automated DNA Sequencing and Analysis 1994, P51
(10) Myers, E; Science 2000, V287, P2196 MEDLINE
(12) Strathmann, M; Proc Natl Acad Sci USA 1991, V88, P1247 CAPLUS
(13) Veklerov, E; Computer Applications in the Biosciences 1995, V11, P173 CAPLUS
ALL CITATIONS AVAILABLE IN THE RE FORMAT

ACCESSION NUMBER: 2000:452091   CAPLUS
DOCUMENT NUMBER: 134:217673
TITLE: Fast **probabilistic** analysis of
                       sequence function using **scoring**
                       matrices
AUTHOR(S):   Wu, Thomas D.; Nevill-Manning, Craig G.; Brutlag, Douglas L.
CORPORATE SOURCE: Department of Biochemistry, Stanford University School of Medicine, Stanford, CA, USA

AB   Motivation: We present techniques for increasing the speed of
      sequence anal. using **scoring** matrixes. Our techniques
      are based on calcg., for a given **scoring** matrix, the quantile
      function, which assigns a probability, or p, value to each segmental
      score. Our techniques also permit the user to specify a p
      threshold to indicate the desired trade-off between sensitivity and speed
      for a particular **sequence** anal. The resulting increase in speed
      should allow **scoring** matrixes to be used more widely in
      large-scale sequencing and annotation projects. Results: We develop three
      techniques for increasing the speed of **sequence** anal.:
      probability filtering, lookahead **scoring**, and permuted lookahead
      scoring. In probability filtering, we compute the **score**
      threshold that corresponds to the user-specified p threshold. We use the
      score threshold to limit the no. of segments that are retained in
      the search process. In lookahead **scoring**, we test intermediate
      scores to det. whether they will possibly exceed the **score**
      threshold. In permuted lookahead **scoring**, we **score**
      each segment in a particular order designed to maximize the likelihood of
      early termination. Our two lookahead **scoring** techniques reduce
      substantially the no. of residues that must be examd. The fraction of
      residues examd. ranges from 62 to 6%, depending on the p threshold chosen
      by the user. These techniques permit **sequence** anal. with
      scoring matrixes at speeds that are several times faster than
      existing programs. On a database of 12 177 alignment blocks, our
      techniques permit **sequence** anal. at a speed of 225 residues/s
      for a p threshold of 10-6, and 541 residues/s for a p threshold of 10-20.
      In order to compute the quantile function, we may use either an
      independence assumption or a Markov assumption. We measure the effect of
      first- and second-order Markov assumptions and find that they tend to
      raise the p value of segments, when compared with the independence
      assumption, by av. ratios of 1.30 and 1.69, resp. We also compare our
      technique with the empirical 99.5th percentile **scores** compiled
      in the BLOCKSPLUS database, and find that they correspond on av. to a p
      value of 1.5 .times. 10-5.

REFERENCE COUNT: 33
REFERENCE(S):
                        (1) Altschul, S; J Mol Biol 1990, V215, P403 CAPLUS
                        (2) Altschul, S; Nucl Acids Res 1997, V25, P3389
                            CAPLUS
                        (3) Attwood, T; Prot Eng 1994, V7, P841 CAPLUS
                        (4) Bairoch, A; Nucl Acids Res 1996, V24, P21 CAPLUS
                        (5) Bateman, A; Nucl Acids Res 1999, V27, P260 CAPLUS
                        ALL CITATIONS AVAILABLE IN THE RE FORMAT

L11 ANSWER 5 OF 9 CAPLUS COPYRIGHT 2002 ACS

AB   A review, with 21 refs. Words that are, by some measure, over- or

underrepresented in the context of larger **sequences** have been variously implicated in biol. functions and mechanisms. In most approaches to such anomaly detections, the words (up to a certain length) are enumerated more or less exhaustively and are individually checked in terms of obsd. and expected frequencies, variances, and **scores** of discrepancy and significance thereof. Here we take the global approach of annotating the suffix tree of a **sequence** with some such values and **scores**, having in mind to use it as a collective detector of all unexpected behaviors, or perhaps just as a preliminary filter for words suspicious enough to undergo a more accurate scrutiny. We consider in depth the simple **probabilistic** model in which **sequences** are produced by a random source emitting symbols from a known alphabet independently and according to a given distribution. Our main result consists of showing that, within this model, full tree annotations can be carried out in a time-and-space optimal fashion for the mean, variance and some of the adopted measures of significance. This result is achieved by an ad hoc embedding in statistical expressions of the combinatorial structure of the periods of a string. Specifically, we show that the expected value and variance of all substrings in a given **sequence** of n symbols can be computed and stored in (optimal) $O(n2)$ overall worst-case, $O(nlogn)$ expected time and space. The $O(n2)$ time bound constitutes an improvement by a linear factor over direct methods. Moreover, we show that under several accepted measures of deviation from expected frequency, the candidates over- or underrepresented words are restricted to the $O(n)$ words that end at internal nodes of a compact suffix tree, as opposed to the .THETA.(n2) possible substrings. This surprising fact is a consequence of properties in the form that if a word that ends in the middle of an arc is, say, overrepresented, then its extension to the nearest node of the tree is even more so. Based on this, we design global detectors of favored and unfavored words for our **probabilistic** framework in overall linear time and space, discuss related software implementations and display the results of preliminary expts.

REFERENCE COUNT: 21
REFERENCE(S):
(1) Aho, A; Handbook of Theoretical Computer Science. Volume A: Algorithms and Complexity 1990, P255
(8) Brendel, V; Journal of Biomolecular Structure and Dynamics 1986, V4(1), P11 CAPLUS
(13) Leung, M; Journal of Computational Biology 1996, V3(3), P345 CAPLUS
(18) Schbath, S; J Comp Biol 1997, V4(2), P189 CAPLUS
(19) van Helden, J; J Mol Biol 1998, V281, P827 CAPLUS
ALL CITATIONS AVAILABLE IN THE RE FORMAT

L11 ANSWER 6 OF 9   CAPLUS COPYRIGHT 2002 ACS
ACCESSION NUMBER: 1999:102048 CAPLUS
DOCUMENT NUMBER: 130:135507
TITLE: The **probabilistic** behavior of **sequence** analysis **scores** with application to structural alignment of RNA
AUTHOR(S):   Heyer, Laurie Jones
CORPORATE SOURCE: Univ. of Colorado, Boulder, CO, USA
SOURCE: (1998) 109 pp. Avail.: UMI, Order No. DA9838367
                          From: Diss. Abstr. Int., B 1998, 59(6), 2788
DOCUMENT TYPE: Dissertation
LANGUAGE: English
AB   Unavailable

L11 ANSWER 7 OF 9   BIOSIS COPYRIGHT 2002 BIOSIS   DUPLICATE 2
ACCESSION NUMBER: 1997:220941 BIOSIS
DOCUMENT NUMBER: PREV199799512657
TITLE: Automated **probabilistic** method for assigning

AB We present a computer **algorithm** for the automated assignment of polypeptide backbone and 13C-beta resonances of a protein of known primary **sequence**. Input to the **algorithm** consists of cross peaks from several 3D NMR experiments: HNCA, HN(CA)CO, HN(CA)HA, HNCACB, COCAH, HCA(CO)N, HNCO, HN(CO)CA, HN(COCA)HA, and CBCA(CO)NH. Data from these experiments performed on glutamine-binding protein are analyzed statistically using Bayes' theorem to yield objective probability **scoring** functions for matching chemical shifts. Such **scoring** is used in the first stage of the **algorithm** to combine cross peaks from the first five experiments to form intraresidue segments of chemical shifts (N-i,H-i-N,C-i-beta,C-i'), while the latter five are combined into interresidue segments (C-i-alpha,C-i-beta,C-i',N-i+1,H-i+1-N). Given a tentative assignment of segments, the second stage of the procedure calculates probability **scores** based on the likelihood of matching the chemical shifts of each segment with (i) overlapping segments; and (ii) chemical shift distributions of the underlying amino acid type (and secondary structure, if known). This joint probability is maximized by rearranging segments using a simulated annealing program, optimized for efficiency. The automated assignment program was tested using CBCANH and CBCA(CO)NH cross peaks of the two previously assigned proteins, calmodulin and CheA. The agreement between the results of our method and the published assignments was excellent. Our **algorithm** was also applied to the observed cross peaks of glutamine-binding protein of Escherichia coli, yielding an assignment in excellent agreement with that obtained by time-consuming, manual methods. The chemical shift assignment procedure described here should be most useful for NMR studies of large proteins, which are now feasible with the use of pulsed-field gradients and random partial deuteration of samples.

L11 ANSWER 8 OF 9 COMPUSCIENCE COPYRIGHT 2002 FIZ KARLSRUHE
AB The title of this book should be Structure and Properties of Game Trees. Its main concern is taming game trees so that the number of positions searched in a game tree is small. It only deals with games where a game tree makes sense. It should be pointed out that this book is a translation from a Russian text that was published in 1978. The first of four chapters is called ''Two-Person Games with Complete Information and the Search of Positions.'' Here the game tree is defined in very general terms. However, most interesting results that follow assume two-player games where moves alternate between players. Alpha-beta pruning is defined, and the number of positions considered in an optimal search with alpha-beta pruning is proved to be O(zn), where n is the total number of positions in the tree. Finally, the expected number of positions considered during a search is derived. The second chapter is called ''Heuristic Methods.'' The importance of the evaluation function is studied and strategies for a good evaluation are mentioned. The next topic is how to look at moves so that the theoretical minimal number of positions considered can be approached. In particular, formulas are derived to show how much bigger the tree can get depending on the kind of deviation from the theoretical optimum. Move ordering is considered, and the expense of move ordering is discussed. Next, the importance of expanding the tree at unstable positions is explained. That is, the evaluation function should not be applied until unstable positions have

settled. Finally, suggestions for introducing strategy are provided. Chapter 3 is ''The Method of Analogy.'' This is the longest chapter and deals with the subject of when an evaluation for a move can be reused in another position. Long and complicated conditions are developed that attempt to define when a sequence of moves does not influence the evaluation of another specific move. The last chapter is called ''Algorithms for Games and Probability Theory.'' Quoting from the preface: ''This approach has four aspects: a) the methods for formulating the elementary stochastic hypotheses and calculating the probability of correctly scoring a given position and finding the best moves; b) the methods for statistical testing of our hypotheses; c) the construction of more effective methods for computing the score and finding the best moves in a given position, on the basis of an analysis of a stochastic model of the game; d) the probabilistic approach to the programming of games with complete information.'' Philosophically, the authors believe there is no reason for a program to behave like a human. They simply want to use the computer to solve a problem. They also claim that knowledge about the game being programmed is not vital and, in fact, can be detrimental. It is more important to focus on the underlying algorithm. I found this book tedious. There is no real flow that would lead the reader from topic to topic. Instead, we are taken from one equation about trees to the next, often with little motivation as to why we should be interested in these equations. The authors developed the material for this book while working on chess-playing programs, yet very little practical advice can be found. This is especially disturbing since the authors point out that ideas about games must be tested in actual programs to determine their fruitfulness. Nevertheless, the theoretical results are interesting and probably can be applied when properly interpreted. There is a complete (but dated) bibliography, which is well worth perusing. The two-page index is too small, however. Many important terms are not included in the index, forcing the reader to search through the text to find the definitions. -Richard J. Lorentz, Northridge, C

L11   ANSWER 9 OF 9   COMPUSCIENCE   COPYRIGHT   2002 FIZ KARLSRUHE
AB   As even the casual reader of the New York Times or Scientific American is now aware, the question of determining when a given positive integer is prime, a problem in pure mathematics considered old and hoary when Euclid was a pup, is intimately tied to the design of modern highly secure cryptographic systems. Abstract algebra and number theory, long scorned by computer scientists as ''generalized abstract nonsense,'' have now acquired the new respectability of being ''applicable mathematics'' for which funding might actually be available, even from those well-endowed agencies which prefer to remain in the shadows. The book under consideration is intended for readers having a mathematical background equal at least to that of a first-year graduate student, and having a mathematical sophistication to match; it is definitely not for the casual reader. The definitions given are exact, and the proofs are rigorous. However, in addition, algorithms for the various procedures developed are given and analyzed as explicitly as possible. This makes it a good and valuable book for pure mathematicians and students of mathematics who are either interested (or eager) to know to what use their work can be put or who are scouting out new directions in which to develop their theories. Exercises (mostly theoretical) are also provided. The book is divided into six chapters. Of them, two are surveys of mathematical background material: Chapter 1 is a quick review of number theory and of certain efficient number-theoretic computational procedures, and Chapter 3 is an even briefer introduction to probability theory. Chapter 2, the basis for the book, concentrates on primality testing, with special emphasis on various efficient algorithms (deterministic and probabilistic) for datermining whether certain positive integers are prime. The first application of these results-the generation of pseudorandom generators-is the subject of Chapter 4. Here the author concentrates on the generation

of pseudoran om sequences and introduces the notion of polynomial time unpredictability as a measure of the randomness of such sequences. Applications to the construction of cryptographic protocols are also given. In Chapter 5, the author discusses several public-key cryptosystems based on primality. Finally, in Chapter 6, he presents the framework for a general mathematical theory for the analysis of pseudorandom generators and public-key cryptosystems. This chapter points the way to new avenues of research-both theoretical and practical-which are sure to prove fruitful in the coming years. -Jonathan Golan, Haifa, Israe

=>